Corrections to *Aggregate Cyber-Risk Management in the IoT Age: Cautionary Statistics for (Re)Insurers and Likes*

Ranjan Pal, *Member, IEEE*, Ziyuan Huang, *Student Member, IEEE*, Xinlong Yin, *Student Member, IEEE*, Sergey Lototsky, *Member, IEEE*, Swades De, *Senior Member, IEEE*, Sasu Tarkoma, *Senior Member, IEEE*, Mingyan Liu, *Fellow, IEEE*, Jon Crowcroft, *Fellow, IEEE*, and Nishanth Sastry, *Senior Member, IEEE*

As authors of our recently accepted article: *Aggregate Cyber-Risk Management in the IoT Age: Cautionary Statistics for (Re)Insurers and Likes*, published in the IEEE IoT Journal, we regret that we have found a few errors in the numerical evaluation setup of the works in [1] and [2] that we had borrowed for our accepted paper. In this correction statement, we describe the errors in detail, correct it, and present our revised results with a renewed experimental setup, hoping it to replace the existing incorrect numerical results in the accepted paper. We apologize for the inconvenience caused to the reader. We emphasize that the numerical evaluation section does not in any way hamper the theoretical contributions in this article, and was initially only meant to provide some empirical evidence for whether the theory proposed in this article generalizes to behavioral settings introduced in [2].

Data Set Forming the Basis of Our "Faulty" Numerical Evaluation

Eling and Schnell [1] considered 1553 cyber losses between 1995 and 2014 extracted from the SAS OpRisk database. We, in [3], did not have access to this paid data set (the data set is not sold anymore by SAS), and apologetically borrowed (assuming correctness) the statistical parameters obtained by Eling and Schnell [1] along with their prospect-theoretic setup, to run our numerical experiments.

Manuscript received April 21, 2021; accepted April 29, 2021. Date of current version July 7, 2021. *(Corresponding author: Ranjan Pal.)*

Ranjan Pal, Ziyuan Huang, Xinlong Yin, and Mingyan Liu are with the Department of Electrical Engineering and Computer Science, University of Michigan at Ann Arbor, Ann Arbor, MI 48109 USA (e-mail: palr@umich.edu; ziyuanh@umich.edu; connory@umich.edu; mingyan@umich.edu).

Sergey Lototsky is with the Department of Mathematics, University of Southern California, Los Angeles, CA 90007 USA (e-mail: lototsky@umich.edu).

Swades De is with the Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi 110016, India (e-mail: swadesd@ee.iitd.ac.in).

Sasu Tarkoma is with the Department of Computer Science, University of Helsinki, 00100 Helsinki, Finland (e-mail: sasu.tarkoma@helsinki.fi).

Jon Crowcroft is with the Computer Laboratory, University of Cambridge, Cambridge CB2 1TN, U.K., and also with the Communications Group, Alan Turing Institute, London NW1 2DB, U.K. (e-mail: jac22@cam.ac.uk).

Nishanth Sastry is with the Department of Informatics, King's College London, London WC2R 2LS, U.K., and also with the Department of Computer Science, University of Surrey, Guildford GU2 7XH, U.K. (e-mail: nishanth.sastry@kcl.ac.uk).

Digital Object Identifier 10.1109/JIOT.2021.3077963

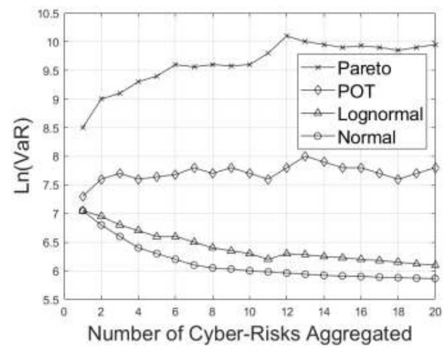

Fig. 1. Fig. 2 in [3].

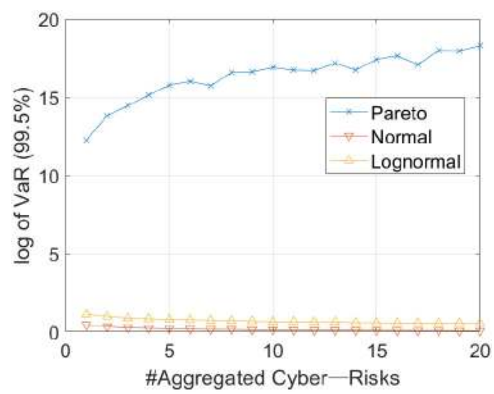

Fig. 2. Revised Fig. 2(a) for [3].

Description of Them Issue in the Borrowed Numerical Evaluation Setup

We are unable to generalize the results for the prospect-theoretic behavioral setup proposed in [1], for a broader set of feasible model parameters. This is the main motivation for us to file the correction. On a closer and repeated look, we are not sure whether the parameters (e.g., Pareto Index of 0.62) proposed for the numerical evaluation setup mentioned in [1] are derived accurately in [1]—and due to lack of access to their data set, it is hard for us to verify the parameters. To detail further, in order to analyze which distribution describes the data best, Eling and Schnell [1] compared several goodness-of-fit statistics for several widely used distributions. They arrive at

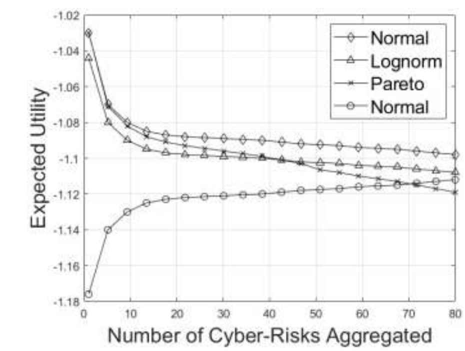

Fig. 3. Fig. 4(a) in [3].

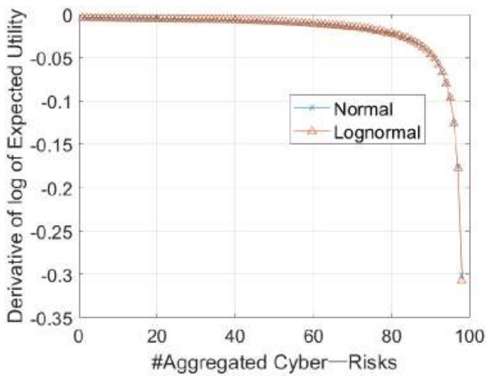

Fig. 4. Revised Fig. 4(a) for [3] for non-heavy-tailed distributions.

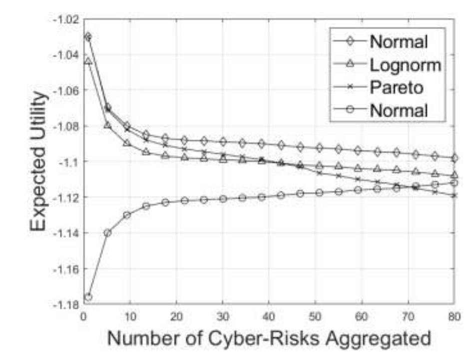

Fig. 5. Fig. 4(a) in [3].

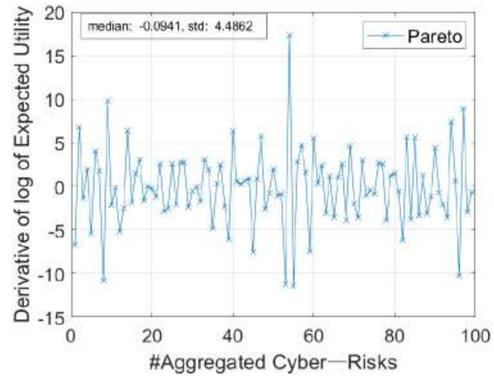

Fig. 6. Revised Fig. 4(b) for [3] for the Pareto heavy-tailed distribution.

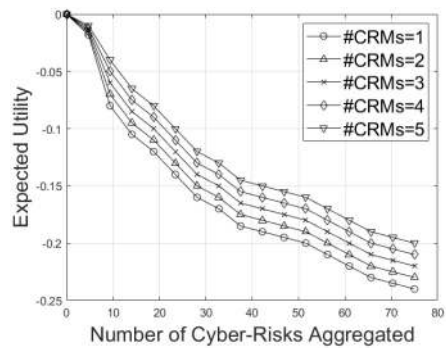

Fig. 7. Fig. 6(a) in [3].

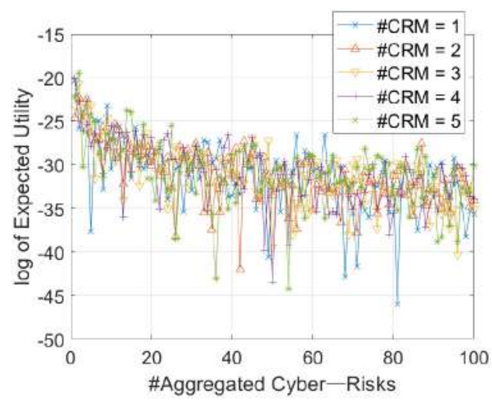

Fig. 8. Revised Fig. 6(a) for [3].

the conclusion (perhaps by mistake) on [1, p. 5] that the data are indeed heavy tailed for which the *expectation and variance, both do not exist.* The latter point is not true in practice for the data set at hand, and had escaped our eyes initially. Fig. 4 in [1] confirms this fact, contrary to the claim made in [1, p. 5], that the expected value of the cyber-risk distribution indeed exists and is not undefined—with the Pareto distribution (a heavy-tailed distribution) being the best fit. We strongly feel there is enough confusion in the evaluation efforts of [1] for us not to be able to generalize our results after borrowing their setting.

Revisiting Results With Renewed Numerical Evaluation Setup

We rerun Monte Carlo simulations with cyber-breach data reported through the *Privacy Rights Clearinghouse* data set (a free public data set posted in 2017 with 9015 breach records), that we recently got access to. Through a goodness-of-fit statistics, we fit a heavy-tailed Pareto distribution with a finite mean and an index of 0.1862. Like in [3], we study the performance of the expected utility, VaR, and the CVaR risk measures with respect to the number of cyber-risks aggregated. Due to lack of data on interdistributional tail dependencies, unlike [1] and [3], we refrain from assuming any particular dependency based on the experimental setup in [1]. On a similar note, we refrain from assuming any particular behavioral prospective-theoretic parameter, unlike in [1] and [3], to study the effect of firm psychology on cyber-risk aggregation propensities. We simply observe the variation of standard cyber-risk measures with the increasing number of "to be aggregated" independent identically distributed (heavy-tailed) cyber-risks, and discover

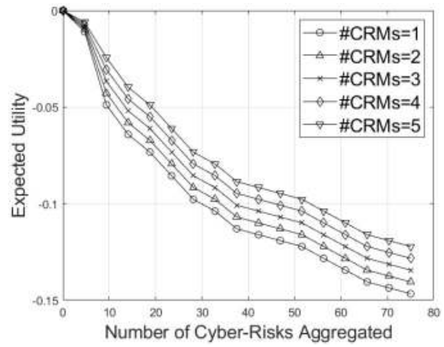

Fig. 9. Fig. 6(a) in [3].

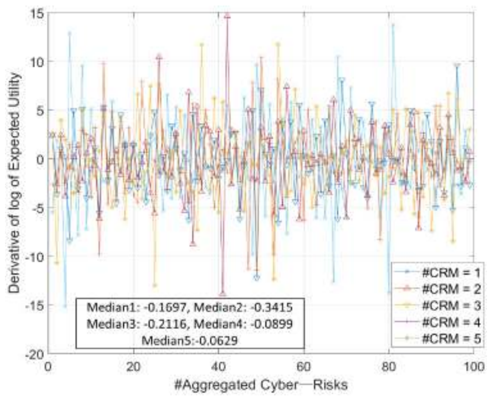

Fig. 10. Revised Fig. 6(b) for [3].

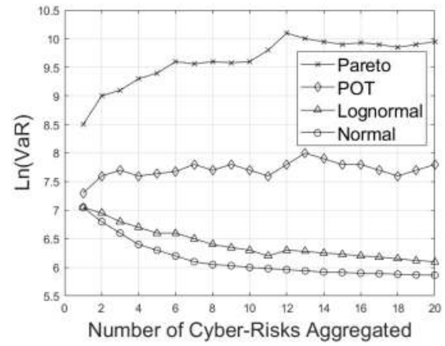

Fig. 11. Fig. 2 in [3].

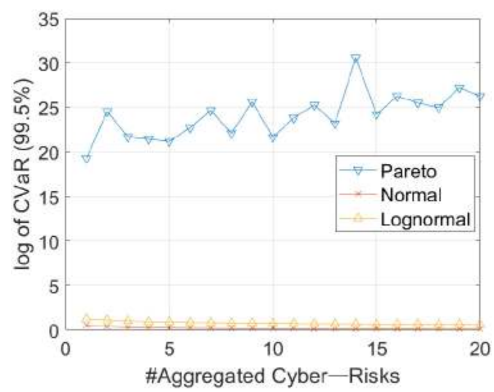

Fig. 12. Revised Fig. 2(b) for [3].

(not-yet-documented) interesting ways in which our proposed theory is validated empirically.

FIGURES

We replot (with a brief explanation where necessary) some of the figures in [3] with our renewed experimental setup. For each pair of figures, the one on the left are from [3], and is replaced/corrected with the corresponding figure on the right.

Fig. 3 of [3] has been omitted in our correction, due to lack of data on interdistributional dependencies.

Figs. 4 and 6 indeed validate the theory proposed in [3]—however, not in a "smooth" fashion for heavy-tailed cyber-risks as experimentally showcased in [3] induced by the experimental setup of [1]. Via Monte Carlo simulations, we show that the rate of decrease (corroborated in theory) in expected utility with heavy-tailed cyber-risk distributions fluctuates (instead of exhibiting monotonic behavior)—however, on average is borderline negative with a high standard deviation (see Fig. 6). This high deviation in the rate change is absent for non-heavy-tailed cyber-risk distributions (see Fig. 4).

The expected utility for a CRM having the support of reinsurers decreases with an increasing number of cyber-risks to be aggregated (see Fig. 8) and follows the trend of Fig. 6(a) in [1] and [3]—however, the rate of decrease on average is approximately a constant near zero for large reinsurance support (see Fig. 10). This implies that reinsurance checks the drop in expected utility on cyber-risk aggregation (also shown via Fig. 8).

Fig. 5 of [3] is plotted correctly and stays as it is.

REFERENCES

[1] M. Eling and W. Schnell. (2020). *Extreme Cyber Risks and the Nondiversification Trap*. [Online]. Available: https://www.alexandria.unisg.ch/publications/260004

[2] M. Eling and J. Wirfs, "What are the actual costs of cyber risk events?" *Eur. J. Oper. Res.*, vol. 272, no. 3, pp. 1109–1119, 2019.

[3] R. Pal *et al.*, "Aggregate cyber-risk management in the IoT age: Cautionary statistics for (Re)Insurers and likes," *IEEE Internet Things J.*, vol. 8, no. 9, pp. 7360–7371, May 2021.